Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A microelectronic circuit arrangement intended for protecting at least one electronic component against illicit manipulation and/or unauthorized access, having at least one activating unit for checking that at least one activating condition is met and for activating at least one preventing unit that is also associated with the circuit arrangement and that is connected to the activating unit, by means of which preventing unit the component can be at least partly de-activated and/or at least partly destroyed in the event of illicit manipulation and/or unauthorized access;

characterized in that the preventing unit is arranged

(j=1) to prevent an internal oscillator from beginning to oscillate;

(j=2) to prevent an oscillator for an external clock signal from beginning to oscillate;

(j=4) to prevent the build-up of a high voltage; and

(j=7) to switch on an increased current drain in the operating state or the quiescent state.

2. (currently amended) A circuit arrangement as claimed in claim 1, characterized in that the preventing unit is constructed

in analog circuit technology or

in at least directly digital circuit technology, in the form of ~~for example~~ at least one fuse and/or at least one antifuse.

3. (previously presented) A circuit arrangement as claimed in claim 1, characterized in that the activating unit is arranged

(i=1) to recognize once or more than once at least one illicit command,

(i=2) to recognize a multiplicity of different illicit operations,

(i=3) to issue at least one specific activating command

(i=4) to issue at least one activating command together with data that addresses a plurality of components by means of at least one group coding, or an individually coded component, and/or

(i=5) to recognize once or more than once at least one physical attack on the components, by means of sensor circuitry belonging to the component that is intended for this purpose.

4. (currently amended) A circuit arrangement as claimed in claim 1, characterized in that the preventing unit is arranged

~~(j=1) to prevent an internal oscillator from beginning to oscillate~~

~~(j=2) to prevent an oscillator for an external clock signal from beginning to oscillate,~~

(j=3) to switch off a high-voltage limiter, in particular by means of permanent programming,

~~(j=4) to prevent the build-up of a high voltage,~~

(j=5) to reprogram the allocation of addresses and/or the allocation of data, and/or

(j=6) to load the memory element of the component with illicit values of data, ~~and/or~~

~~(j=7) to switch on an increased current drain in the operating state or the quiescent state~~.

5. (currently amended) A method of protecting at least one electronic component against illicit manipulation and/or unauthorized access, characterized by the following method steps:

(i) checking that at least one activating condition is met by means of at least one activating unit,

(ii) in the event of illicit manipulation of the component and/or unauthorized access to the component activating at least one preventing unit that is connected to the activating unit, and

(iii) at least partly de-activating the operation of the component and/or at least partly destroying the component ~~(200)~~, by means of the preventing unit;

characterized in that the at least partial de-activation of the operation of the component and/or the at least partial destruction of the component is carried out by

(j=1) preventing an internal oscillator from beginning to oscillate;

(j=2) preventing an oscillator for an external clock signal from beginning to oscillate;

(j=4) preventing the build-up of a high voltage; and

(j=7) switching on an increased current drain in the operating state or the quiescent state.

6. (previously presented) A method as claimed in claim 5, characterized in the check on whether the activating condition is met is made by analyzing at least one data stream applied from outside or by signals from the internal sensor circuitry of the component.

7. (currently amended) A method as claimed in claim 5 ~~or 6~~, characterized in that, if the activation condition is met

recognition of this fact and the desired effects it is to have are placed in store in coded form in at least one memory element that is used for starting-up the component, and

the start-up, which initiates the appropriate actions, is repeated.

8. (previously presented) A method as claimed in claim 5, characterized in that the activation takes place

(i=1) as a result of the recognition once or more than once of at least one illicit command,

(i=2) as a result of the recognition of a multiplicity of different illicit operations,

(i=3) as a result of the issue of at least one specific activating command,

(i=4) as a result of the issue of at least one activating command together with data that addresses a plurality of components by means of at least one group coding, or an individually coded component, and/or

(i=5) as a result of the recognition once or more than once of at least one physical attack on the component, by means of sensor circuitry belonging to the component that is intended for this purpose.

9. (currently amended) A method as claimed in claim 5, characterized in that the at least partial de-activation of the operation of the component and/or the at least partial destruction of the component is carried out by

~~(j=1) preventing an internal oscillator from beginning to oscillate,~~

~~(j=2) preventing an oscillator for an external clock signal from beginning to oscillate,~~

(j=3) switching off a high-voltage limiter, in particular by means of permanent programming,

~~(j=4) preventing the build-up of a high voltage,~~

(j=5) reprogramming the allocation of addresses and/or the allocation of data, and/or

(j=6) loading at least one memory element of the component with illicit values of data, ~~and/or~~

~~(j=7) switching on an increased current drain in the operating state or the quiescent state~~.

10. (currently amended) Use of at least one circuit arrangement as claimed in claim 1 ~~and/or of the method as claimed in claim 5~~ for the self-destruction of at least one integrated circuit in the event of unauthorized use in the field or of an illicit attempt to analyze the integrated circuit by at least partial reverse preparation.

11. (new) Use of at least one circuit arrangement as claimed in claim 5 for the self-destruction of at least one integrated circuit in the event of unauthorized use in the field or of an illicit attempt to analyze the integrated circuit by at least partial reverse preparation.

12. (new) A microelectronic circuit arrangement intended for protecting at least one electronic component against illicit manipulation and/or unauthorized access, having at least one activating unit for checking that at least one activating condition is met and for activating at least one preventing unit that is also associated with the circuit arrangement and that is connected to the activating unit, by means of which preventing unit the component can be at least partly de-activated and/or at least partly destroyed in the event of illicit manipulation and/or unauthorized access;

characterized in that the preventing unit is arranged (j=4) to prevent the build-up of a high voltage.